



openHPI – Sicherheit im Internet Malware: Schutzmaßnahmen

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Potsdam

Regelmäßige Datensicherung – Backup (1/2)

Angriffe im Internet durch Malware verursachen sehr oft
Verlust bzw. die **Beschädigung von Daten**

- Bei Datenverlust durch Viren, Ransomware oder Beschädigung des Betriebssystems können Daten aus vorher angelegten Sicherungskopien - „**Backups**“ - wiederhergestellt werden
- Wichtige und persönliche Daten müssen deshalb regelmäßig gesichert werden
- Systeme bieten automatische Datensicherung in vordefinierten Zeitabständen an
- Datensicherungen auf externen Medien speichern
- Externe Medien physisch getrennt vom Computer aufbewahren
 - Falls Angreifer eigenen Computer komplett übernehmen, haben sie keine Möglichkeit, auf Datensicherung zuzugreifen

Regelmäßige Datensicherung – Backup (2/2)

Angriffe im Internet durch Malware verursachen sehr oft

Verlust bzw. die **Beschädigung von Daten**

Daten können auch **online** (z.B. in der Cloud) abgelegt werden

- Hierzu ist eine sichere Zugangskontrolle zu den persönlichen Daten erforderlich
- Verschlüsselung der Backups ist empfehlenswert
- Keine ständige Verbindung aufrechterhalten zu Online-Sicherungsmedien, da lokale Änderungen direkt in den Onlinespeicher übernommen werden
- Speicherung von verschiedenen Versionen ermöglicht es, gegebenenfalls spezifische Änderungen rückgängig zu machen

Programm-Updates (1/2)

Programm-Updates dienen dazu, bekannt gewordene Schwachstellen in der Software zu beheben und dadurch Sicherheitsrisiken zu beseitigen

- Verwendung (älterer) Software-Versionen, die nicht upgedatet wurden, stellt somit ein Sicherheitsrisiko dar wegen der erhöhten Missbrauchsgefahr der nun auch öffentlich bekannten Schwachstellen

Updates stets durchführen, sobald sie verfügbar sind:

- Hersteller finden nicht alle Lücken während der Testphase. Viele Sicherheitslücken in Programmen werden oft erst nach der Veröffentlichung entdeckt, z.B. durch
 - Analysen externer Experten, bekannt gewordene Angriffe, ...
- Bekannt gewordene Sicherheitslücken können meist schon durch kleinere Updatepakete geschlossen werden

- Oftmals geben moderne Programme von selbst automatisch Hinweise auf vorhandene Updates
- Darüber hinaus gibt es Anwendungen, die automatisch nach Updates für die installierte Software suchen
- Auch einige Antivirusprogramme überprüfen Aktualität der installierten Software



Doch bei allen Updates gilt:

- Überprüfung der Vertrauenswürdigkeit der Quelle und des Updates sind unumgänglich
- Ansonsten können Updates selbst zur Quelle neuer Angriffspunkte und Ursache für die Installation von Schadsoftware werden ...

Virens Scanner und **Antivirussoftware** bieten Verfahren zum Detektieren von Malware

- Können neben Viren meist auch Würmer, Trojaner, Spyware und andere Schadsoftware erkennen
 - Daher können diese Produkte besser auch als **Anti-Malwaresoftware** bezeichnet werden
- Einige diese Produkte überwachen auch Internetverbindungen und warnen vor unsicheren Internetseiten
- Sind mittlerweile als **zwingend notwendiger Bestandteil** von mit dem Internet verbundenen Systemen anzusehen und in diese zu integrieren

Anti-Malwaresoftware basiert auf zwei unterschiedlichen Erkennungsmethoden:

■ Signaturen

- Signaturen werden durch Analyse von Malware gewonnen und „beschreiben“ markante Charakteristika der Malware
- Dateien werden auf diese charakteristischen Merkmale hin überprüft und entsprechend eingestuft

■ Anomalien

- Normaler bzw. „gutartiger“ Zustand des Systems wird erfasst und dann ständig mit aktuellem Zustand verglichen
- Bei starker Abweichung des aktuellen Zustands wird eine Warnung erzeugt
- Ermöglicht die Erkennung auch unbekannter Malware, jedoch sind Anomalie-basierte Methoden oft ungenauer

- Anti-Malwaresoftware muss stets auf neuestem Stand gehalten werden
 - Ständig aktualisierte Virendefinitionen und -signaturen ermöglichen auch das Auffinden neuer Viren und Malware
- Müssen im Idealfall alle Datenquellen nach Viren durchsuchen
 - Festplatten, Wechselmedien (CD, USB-Sticks,...), Netzwerkverbindungen, ...
- Meist entfernen Virens Scanner gefundene Schadsoftware automatisch, doch wenn häufiger Viren gefunden werden, kann eine manuelle Untersuchung der Ursache weiterhelfen
- Infizierte Systeme sind meist langsamer, unsicher oder fallen komplett aus. Daher sind die Warnungen vor Viren / Malware ernst zu nehmen und das Problem so schnell als möglich zu beheben

Firewalls überwachen alle ein- und ausgehenden Netzwerkverbindungen und den darüber laufenden Datenverkehr

- Können unberechtigte Verbindungsversuche unterbinden
- Bieten zusätzlichen Schutz gegen Angriffe, wie z.B. Angriffe durch Backdoors oder Botnets
 - Bei jedem der Angriffe wird eine Verbindung zum/vom Angreifer aufgebaut, die vom Nutzer nicht genehmigt wurde. Diese Verbindung muss verhindert oder ein Alarm ausgelöst werden
- Lokale Firewall agiert nur auf dem System, auf dem sie installiert ist
- Netzwerkfirewall prüft den gesamten Netzwerkverkehr und ist meist auf Verbindungsknoten zwischen einem lokalen Netzwerk und dem Internet installiert

Funktion einer Firewall wird über sogenannte Regeln gesteuert

- Regeln definieren, welche Verbindungen zulässig sind und welche nicht
- Regeln können spezifisch für einzelne Anwendungen, Protokolle, Ports und Adressen formuliert werden und definieren exakt, was zulässig ist und was nicht
- Falls eine Regel auf ein Netzwerkpaket zutrifft, können verschiedene Aktionen ausgeführt werden
 - Datenpaket kann modifiziert oder ganz geblockt werden
 - Warnungen können angezeigt werden,
 - ...
- **Windows Firewall** ist standardmäßig aktiv
- Linux stellt mit **iptables** ebenfalls eine Firewall bereit

Gesundes Misstrauen (1/2)

Gesundes Misstrauen ist wirkungsvollste Schutzmaßnahme vor Infektionen mit Malware

- Die besten Warn- und Schutzmechanismen sind hinfällig, wenn der Benutzer nicht-vertrauenswürdige Inhalte öffnet
- Beim Installieren neuer Software immer Hersteller und Herkunft überprüfen
- Signatur der zu installierenden Software / Updates verifizieren (kann automatisch erfolgen)
- Falls Warnung vorliegt, manuelle Überprüfung notwendig
- Nur Software installieren, die wirklich gebraucht wird
 - unnötige Anwendungen, Addons, Zusatzfeatures, optionale Plugins nicht installieren - sie bieten eine unnötige Angriffsfläche für Angreifer

Gesundes Misstrauen (2/2)

- Aktive Inhalte (Flash, Java, Active X) im Web-Browser standardmäßig abstellen, da diese eine Reihe verschiedener Angriffs- und Einbruchsmöglichkeiten bieten
- „Cookies“ nur für vertrauenswürdige Seiten verwenden
- Email Anhänge nur öffnen, wenn
 - Absender bekannt ist und Text dem Absender zuordenbar ist
 - eine Email mit Anhang auch erwartet wurde
- Ruhe bewahren bei Onlinewarnungen und Aufforderungen zur Entrichtung von Strafgeldern
- Installierte Software überprüfen und alle nicht genutzten, überflüssigen Programme entfernen